

REMARKS/ARGUMENTS

Claim 1 was pending. By this amendment, Applicant submits claims 2-5 for entry and examination, so claims 1-5 will be pending.

In the Office Action, the Examiner rejected claim 1 under 35 USC §102(e) as being anticipated by U.S. Patent No. 5,548,648 to Yorke-Smith. Applicant respectfully traverses that rejection and requests reconsideration and withdrawal of the rejection. Further, Applicant respectfully requests entry and allowance of new claims 2-5.

Claim 1 is allowable over Yorke-Smith as that reference fails to disclose or suggest each element of claim 1. For example, the reference fails to disclose or suggest "using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first portion..." as claimed. In making the rejection, the Examiner asserted that Yorke-Smith showed a second portion of a message overlapping a first portion of the message, identifying "transition regions" that constitute overlap regions in the bits referring to both the second and first encrypted data segment are to be found there. It is not apparent where Yorke-Smith mentions overlaps, overlap regions or transition regions.

As Yorke-Smith's Fig. 3 clearly shows, EDB₁ and CB₂ do not overlap. EDB₁ ends and then CB₂ begins. As set out in the example description at column 2, lines 50-64, the control blocks are associated with encrypted data blocks and a control block contains information usable to decrypt encrypted data blocks. Nothing there suggests that the control block of one data block is at all included with data encrypted for another data block. This is further supported by the source code included with the Yorke-Smith specification, which appears to indicate that each data block is processed on its own, without data overlapping from another data block.

As further support for the proposition that a control block does not overlap an encrypted data block, the Examiner's attention is directed to Yorke-Smith's Fig. 6. As shown there, in step 610, a control block for a data block being decrypted is obtained from the input file. If the control block were somehow overlapping earlier data, such as a prior encrypted data block,

the control block for the later data block would already be available and would not need to be read in from the input file.

Therefore, for at least the reasons stated above, Applicant submits that claim 1 is allowable over Yorke-Smith.

Claim 2, and claims 3-4 dependent therefrom, are also allowable over Yorke-Smith as they contain elements not disclosed or suggested by that reference. For example, claim 2 recites subdividing a designated cipher block into a first portion and a second portion, which is not disclosed or suggested by the reference. Claim 2 also recites encrypting the second portion and a residual portion, which is also not disclosed or suggested by the reference. Therefore, claims 2-4 are allowable over the cited reference.

Claim 5 is also allowable over Yorke-Smith as it contains elements not disclosed or suggested by that reference. For example, claim 5 recites subdividing a designated cipher block into a first portion and a second portion and encrypting the second portion and a residual portion, which are not disclosed or suggested by the reference.

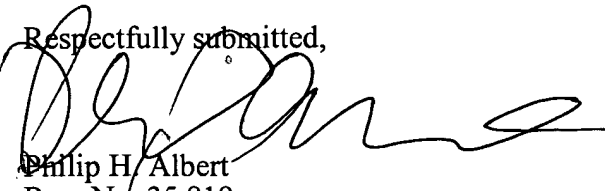
CONCLUSION

In view of the foregoing, Applicant believes all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Dated: 3/17/04

Respectfully submitted,


Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200 Fax: 415-576-0300
PHA:jtc
60143883 v1